

Japanese Patent Application Laid-open No. Hei 10-23548

Laid-open Date: January 23, 1998

[0046] Next, a schematic configuration of a communication system in which the portable storage device 1 and other plural electronic equipments transmit and receive signals wirelessly therebetween is shown in Fig. 2.

[0047] The portable storage device 1 performs wireless transmissions/receptions of encrypted signals to/from various electronic equipments, such as a facsimile machine 301, a so-called tower-type computer device 302, a high-performance and large-scale computer device 303, a so-called handheld computer device 304, a projector device 305, and a notebook-type personal computer device (hereinafter referred to as a PC) 306.

[0048] The electronic equipments having received the encrypted signals transmitted from the portable storage device 1 decrypt the encrypted signals to restore original data, and print or process the data.

[0049] As a method of encrypting/decrypting the data, "KEY PREDISTRIBUTION SYSTEM (hereinafter referred to as KPS): A method of sharing cryptographic key without communication," which is published in IEICE TRANSACTIONS of The Institute of Electronics, Information and Communication Engineers; A Vol. J71-A No. 11, pp. 2046-2053, November 1988, is used. In the method of

encrypting/decrypting the data by use of this KPS, the cryptographic key for use in encrypting and decrypting the data is previously shared among the electronic equipments which transmit/receive the data. The electronic equipments transmitting the data encrypt the data by use of the cryptographic key, and the electronic equipments receiving the data decrypt the received encrypted signals by use of the cryptographic key.

[0050] In order to create the cryptographic key for use in this KPS, each of the portable storage device 1, the facsimile machine 301, the tower-type computer device 302, the high-performance and large-scale computer device 303, the handheld computer device 304, the projector device 305, and the PC 306 includes unique identification information (hereinafter, referred to as a unique ID), and a unique and secret algorithm. Specifically, the portable storage device 1 stores the unique ID and the unique and secret algorithm in a memory provided in the encryption/decryption unit 20.

[0051] When a signal is to be transmitted/received between two electronic equipments in the communication system, first, the unique IDs are mutually transmitted/received, and the unique ID of the electronic equipment to which the signal should be transmitted is stored. Next, one of the electronic equipments which transmits the signal creates a cryptographic key by use of the received unique ID of the other electronic equipment and a secret

algorithm unique to itself, and encrypts the data by means of a cryptographic key program using this cryptographic key. Then, the one electronic equipment transmits an encrypted signal based on this encrypted data to the other electronic equipment. Moreover, the other electronic equipment also creates a cryptographic key by use of the received ID unique to the one electronic equipment and a secret program unique to itself, and decrypts the received encrypted signal according to a cryptographic key program using this cryptographic key to restore the original data.

[Fig. 2] A diagram for explaining transmissions/receptions of signals between the portable storage device and other electronic equipments.

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-023548

(43)Date of publication of application : 23.01.1998

(51)Int.Cl.

H04Q 7/38  
 G06F 9/06  
 G06K 17/00  
 G09C 1/00  
 H04L 9/08  
 // G06F 12/14

(21)Application number : 08-195709

(71)Applicant : SEIKO EPSON CORP

(22)Date of filing : 05.07.1996

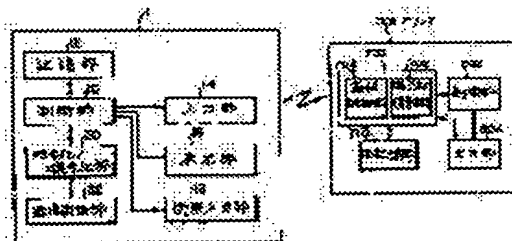
(72)Inventor : MATSUI TETSUYA

## (54) PORTABLE COMMUNICATION DEVICE AND PORTABLE STORAGE DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a portable communication device and portable storage device which are portable electronic equipment equipped with various functions and can send and receive high-safety signals to and from other electronic equipment.

SOLUTION: Data read out of a storage part 12 are sent to a ciphering/deciphering part 20 under the control of a control part 10. The ciphering/deciphering part 20 generates a cipher key by using the ID characteristic of the other electronic equipment to which signals should be sent and the secret program characteristic of this equipment and ciphers the said data by a cipher key program using this cipher key. The ciphered data are sent to the said opposite electronic equipment through a communication control part 22.



## LEGAL STATUS

[Date of request for examination]

03.07.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's

decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平10-23548

(43)公開日 平成10年(1998) 1月23日

(51)Int.Cl. <sup>6</sup>	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 Q 7/38			H 0 4 B 7/26	1 0 9 S
G 0 6 F 9/06	5 5 0		G 0 6 F 9/06	5 5 0 Z
G 0 6 K 17/00			G 0 6 K 17/00	E
G 0 9 C 1/00	6 3 0	7259-5 J	G 0 9 C 1/00	6 3 0 D
H 0 4 L 9/08			G 0 6 F 12/14	3 2 0 B
審査請求 未請求 請求項の数13 F D (全 12 頁) 最終頁に続く				

(21)出願番号 特願平8-195709

(22)出願日 平成8年(1996) 7月5日

(71)出願人 000002369

セイコーエプソン株式会社

東京都新宿区西新宿2丁目4番1号

(72)発明者 松井 哲也

長野県諏訪市大和3丁目3番5号 セイコーエプソン株式会社内

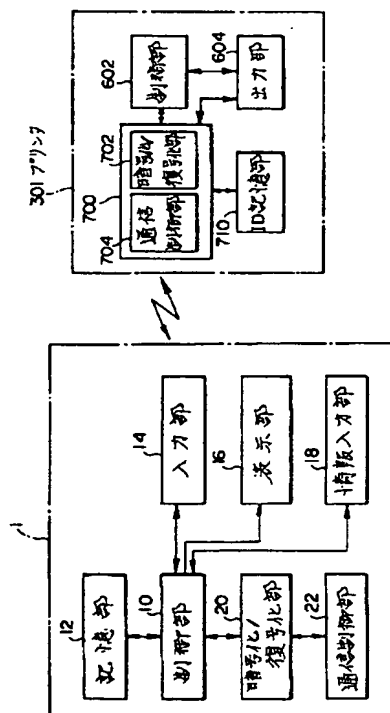
(74)代理人 弁理士 井上 一 (外2名)

(54)【発明の名称】 携帯型通信装置及び携帯型記憶装置

(57)【要約】

【課題】 様々な機能を備える携帯型の電子機器であって、他の電子機器との間で、安全性の高い信号の送受信を行うことができる携帯型通信装置及び携帯型記憶装置を提供すること。

【解決手段】 制御部10の制御により記憶部12から読み出されたデータは、暗号化／復号化部20に送られる。暗号化／復号化部20は、信号を送信すべき他の電子機器の固有のID及び自機の固有の秘密プログラムを用いて暗号鍵を生成し、この暗号鍵を用いた暗号鍵プログラムにより前記データを暗号化する。この暗号化されたデータは、通信制御部22を介して前記他の電子機器に送信される。



## 【特許請求の範囲】

【請求項1】 携帯して信号を送受信する携帯型通信装置において、

他の電子機器との間で、情報を送受信する通信手段と、前記他の電子機器の固有の識別情報及び自機の固有の秘密アルゴリズムを用いてデータを変換し、前記通信手段を介して前記変換したデータによる変換信号を前記他の電子機器に送信する変換手段と、

前記変換信号の送受信動作に先立って、前記通信手段を介して、自機の固有の識別情報を前記他の電子機器に送信し、前記他の電子機器の固有の識別情報を受信する制御手段と、を備えることを特徴とする携帯型通信装置。

【請求項2】 請求項1において、前記変換信号は、暗号化信号であることを特徴とする携帯型通信装置。

【請求項3】 請求項2において、前記変換手段は、前記他の電子機器の固有の識別情報及び自機の固有の秘密アルゴリズムを用いて暗号鍵を生成し、この暗号鍵を用いた暗号鍵プログラムにより前記データを暗号化する暗号化手段であることを特徴とする携帯型通信装置。

【請求項4】 請求項2、3のいずれかにおいて、前記変換手段は、前記他の電子機器から送信された暗号化信号を、前記他の電子機器の固有の識別情報及び自機の固有の秘密アルゴリズムを用いて復号化する復号化手段を含むことを特徴とする携帯型通信装置。

【請求項5】 請求項4において、前記復号化手段は、前記他の電子機器の固有の識別情報及び自機の固有の秘密アルゴリズムを用いて暗号鍵を生成し、この暗号鍵を用いた暗号鍵プログラムにより信号を復号化することを特徴とする携帯型通信装置。

【請求項6】 請求項2～5のいずれかにおいて、携帯型通信装置本体に着脱自在に装着され、固有の識別情報、固有の秘密アルゴリズム、及びデータを記憶する携帯型記憶媒体と、

前記携帯型記憶媒体から前記固有の識別情報、前記固有の秘密アルゴリズム、及び前記データを読み出す情報入力手段と、を含み、

前記制御手段は、前記通信手段を介して、前記情報入力手段からの前記固有の識別情報を前記他の電子機器に送信し、前記他の電子機器の固有の識別情報を受信し、前記暗号化手段は、前記他の電子機器の固有の識別情報及び前記自機の固有の秘密アルゴリズムを用いて暗号鍵を生成し、この暗号鍵を用いた暗号鍵プログラムにより前記データを暗号化して暗号化信号を生成し、前記通信手段は、前記暗号化信号を前記他の電子機器に送信することを特徴とする携帯型通信装置。

【請求項7】 情報を記憶する携帯型記憶装置において、データを記憶する記憶手段と、他の電子機器との間で、情報を送受信する通信手段と、

前記他の電子機器の固有の識別情報及び自機の固有の秘密アルゴリズムを用いて、前記記憶手段に記憶されるデータを変換し、前記通信手段を介して前記変換したデータによる変換信号を前記他の電子機器に送信する変換手段と、

前記変換信号の送受信動作に先立って、前記通信手段を介して、自機の固有の識別情報を前記他の電子機器に送信し、前記他の電子機器の固有の識別情報を受信する制御手段と、を備えることを特徴とする携帯型記憶装置。

【請求項8】 請求項7において、前記変換信号は、暗号化信号であることを特徴とする携帯型記憶装置。

【請求項9】 請求項8において、前記変換手段は、前記他の電子機器の固有の識別情報及び自機の固有の秘密アルゴリズムを用いて暗号鍵を生成し、この暗号鍵を用いた暗号鍵プログラムにより前記データを暗号化する暗号化手段であることを特徴とする携帯型記憶装置。

【請求項10】 請求項8、9のいずれかにおいて、前記変換手段は、前記他の電子機器から送信された暗号化信号を、前記他の電子機器の固有の識別情報及び自機の固有の秘密アルゴリズムを用いて復号化する復号化手段を含むことを特徴とする携帯型記憶装置。

【請求項11】 請求項10において、前記復号化手段は、前記他の電子機器の固有の識別情報及び自機の固有の秘密アルゴリズムを用いて暗号鍵を生成し、この暗号鍵を用いた暗号鍵プログラムにより信号を復号化することを特徴とする携帯型記憶装置。

【請求項12】 請求項10、11のいずれかにおいて、

前記制御手段は、前記暗号化手段で前記記憶手段に記憶するデータを暗号化して暗号化信号を生成し、この暗号化信号を前記通信手段を介して前記他の電子機器に送信した後、前記他の電子機器で処理されたデータを暗号化した暗号化信号を前記通信手段で受信して、前記復号化手段で復号化することを特徴とする携帯型記憶装置。

【請求項13】 請求項10～12のいずれかに記載する携帯型記憶装置を備えて成ることを特徴とする携帯型電話装置。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】 本発明は、携帯して信号を送受信する携帯型通信装置及び情報を記憶する携帯型記憶装置に関する。

## 【0002】

【背景技術】 従来、屋内で、パーソナルコンピュータ装置（以下、PCという）を常時使用している人は、屋外でも使用したいという要望があった。この要望に応じ、PCやプリンタ装置等の電子機器を備え、ユーザーに対して、前記電子機器の使用の提供を専門とする仕事

が開始されている。

【0003】また、将来、例えばコンビニエンスストアや喫茶店等で、PCやプリンタ装置等の電子機器を備え、来店するお客に対して、前記電子機器の使用を提供することが考えられる。

【0004】このとき、ユーザーは、フロッピーディスクやメモリカード等の携帯型記憶媒体を前記コンビニエンスストアや喫茶店に持参して、前記設置されたPCやプリンタ装置に前記携帯型記憶媒体を装着し、前記携帯型記憶媒体に記憶されているデータを処理したり、前記データを他のPC等の電子機器に送信したりすることが可能となる。このように、ユーザーは、前記携帯型記憶媒体のみを持参して、他の電子機器との間で情報の送受信を行うことが可能となる。

【0005】

【発明が解決しようとする課題】ところが、上述したシステムでは、前記携帯型記憶媒体を、PCやプリンタ装置等の電子機器に直接に装着して、その携帯型記憶媒体に記憶されるデータを読み出す。従って、例えば、前記電子機器内にいわゆるコンピュータ・ウィルスが存在する場合には、このコンピュータ・ウィルスが前記携帯型記憶媒体に侵入して、前記携帯型記憶媒体内に記憶されるデータを壊したり、また、前記コンピュータ・ウィルスが侵入した携帯型記憶媒体を他の電子機器で利用した場合、この電子機器内のデータを破壊したりするおそれが生じる。

【0006】さらに、前記携帯型記憶媒体に記憶されるデータを、前記電子機器に内蔵されるハードディスク等の記憶手段に記憶させて処理したときに、その処理したデータを、前記電子機器の記憶手段内に残したままにしてしまうとときがある。このとき、前記処理したデータが秘密データである場合には、その処理したデータを他人に盗まれて、その安全性を保てないおそれが生じる。

【0007】本発明は、このような課題を鑑みてなされたものであり、その目的は、様々な機能を備える携帯型の電子機器であって、他の電子機器との間で、安全性の高い信号の送受信を行うことができる携帯型通信装置及び携帯型記憶装置を提供することにある。

【0008】

【課題を解決するための手段】上記課題を解決するために、請求項1の発明は、携帯して信号を送受信する携帯型通信装置において、他の電子機器との間で、情報を送受信する通信手段と、前記他の電子機器の固有の識別情報及び自機の固有の秘密アルゴリズムを用いてデータを変換し、前記通信手段を介して前記変換したデータによる変換信号を前記他の電子機器に送信する変換手段と、前記変換信号の送受信動作に先立って、前記通信手段を介して、自機の固有の識別情報を前記他の電子機器に送信し、前記他の電子機器の固有の識別情報を受信する制御手段と、を備えることを特徴とする。

【0009】本発明に係る携帯型通信装置は、任意の場所から、他の電子機器に対して、変換したデータを送信する。この携帯型通信装置は、屋内で、所望の他の電子機器にデータを送信する場合の他に、屋外の所望の他の電子機器が存在する場所近傍まで持ち出されて、前記他の電子機器にデータを送信する場合がある。ここで、屋外において送信されるデータは、屋内において送信されるデータよりも、第三者に盗まれるおそれが多くなる。

【0010】このように、屋内及び屋外で送信されるデータを盗まれた場合にも、このデータを解読することは困難であり、より安全性の高いデータを送信することができる。

【0011】請求項2の発明は、請求項1において、前記変換信号は、暗号化信号であることを特徴とする。

【0012】ここで、前記携帯型通信装置及び前記他の電子機器がそれぞれ備える、固有の識別情報及び固有の秘密アルゴリズムは、例えば、電子情報通信学会論文誌

A Vol. J71-A No.11 pp.2046-2053 1988年11月で提案

されている、固有の識別情報及び固有の秘密アルゴリズムを用いて暗号鍵を生成し、この暗号鍵を用いた暗号鍵プログラムによりデータを暗号化する方法である、暗号鍵を通信なしで共有する方法：KEY PREDISTRIBUTION SYSTEM（以下、KPSという）で用いられる、前記固有の識別情報及び前記固有の秘密アルゴリズムである。この暗号鍵を生成するには、携帯型通信装置では、前記他の電子機器の固有の識別情報と自機の固有の秘密アルゴリズムを用い、前記他の電子機器では、前記携帯型通信装置の固有の識別情報及び自機の固有の秘密アルゴリズムを用いる。

【0013】このKPSによって、携帯型通信装置で暗号化されたデータは、前記他の電子機器の固有の識別情報及び自機の固有の秘密アルゴリズムを用いなければ復号化することは困難であり、前記他の電子機器で暗号化されたデータは、前記携帯型通信装置の固有の識別情報及び自機の固有の秘密アルゴリズムを用いなければ復号化することは困難であるので、送信されるデータの安全性を高めることができる。

【0014】請求項3の発明は、請求項2において、前記変換手段は、前記他の電子機器の固有の識別情報及び自機の固有の秘密アルゴリズムを用いて暗号鍵を生成し、この暗号鍵を用いた暗号鍵プログラムにより前記データを暗号化する暗号化手段であることを特徴とする。

【0015】これにより、データを送信するときに、前記固有の識別情報及び前記固有の秘密アルゴリズムを用いて、前記KPSによるデータの暗号化を行うことができる。

【0016】このKPSにより暗号化されたデータは、その送信時に盗まれた場合にも、前記暗号鍵を使用しなければ、復号化することは困難であるので、送信時のデータの安全性を高めることができる。



【0017】請求項4の発明は、請求項2、3のいずれかにおいて、前記変換手段は、前記他の電子機器から送信された暗号化信号を、前記他の電子機器の固有の識別情報及び自機の固有の秘密アルゴリズムを用いて復号化する復号化手段を含むことを特徴とする。

【0018】これにより、他の電子機器から送信される、KPSを用いて暗号化されたデータの暗号化信号を、復号化して、元のデータを復元することができる。

【0019】請求項5の発明は、請求項4において、前記復号化手段は、前記他の電子機器の固有の識別情報及び自機の固有の秘密アルゴリズムを用いて暗号鍵を生成し、この暗号鍵を用いた暗号鍵プログラムにより信号を復号化することを特徴とする。

【0020】前記KPSに用いた復号化を行う際に用いる暗号鍵を、前記送信された他の電子機器の固有の識別情報及び自機の固有の秘密アルゴリズムを用いて生成するので、前記暗号鍵を簡易に生成することができる。

【0021】請求項6の発明は、請求項2～5のいずれかにおいて、携帯型通信装置本体に着脱自在に装着され、固有の識別情報、固有の秘密アルゴリズム、及びデータを記憶する携帯型記憶媒体と、前記携帯型記憶媒体から前記固有の識別情報、前記固有の秘密アルゴリズム、及び前記データを読み出す情報入力手段と、を含み、前記制御手段は、前記通信手段を介して、前記情報入力手段からの前記固有の識別情報を前記他の電子機器に送信し、前記他の電子機器の固有の識別情報を受信し、前記暗号化手段は、前記他の電子機器の固有の識別情報及び前記自機の固有の秘密アルゴリズムを用いて暗号鍵を生成し、この暗号鍵を用いた暗号鍵プログラムにより前記データを暗号化して暗号化信号を生成し、前記通信手段は、前記暗号化信号を前記他の電子機器に送信することを特徴とする。

【0022】この携帯型記憶装置を用いることにより、前記携帯型記憶媒体を前記他の電子機器に装着することなく、前記携帯型記憶媒体に記憶されるデータを前記他の電子機器に送信して、処理することができる。よって、前記携帯型記憶媒体に、前記他の電子機器内のデータが侵入することを防止できる。

【0023】具体的には、例えば、前記他の電子機器内に、いわゆるコンピュータ・ウイルスが存在する場合には、このコンピュータ・ウイルスが前記携帯型記憶媒体に侵入して、この携帯型記憶媒体内のデータを破壊したり、さらには、前記携帯型記憶媒体を装着した電子機器に前記携帯型記憶媒体内のコンピュータ・ウイルスが侵入して、前記電子機器内のデータを破壊したりすることを防止できる。

【0024】請求項7の発明は、情報を記憶する携帯型記憶装置において、データを記憶する記憶手段と、他の電子機器との間で、情報を送受信する通信手段と、前記他の電子機器の固有の識別情報及び自機の固有の秘密ア

ルゴリズムを用いて、前記記憶手段に記憶されるデータを変換し、前記通信手段を介して前記変換したデータによる変換信号を前記他の電子機器に送信する変換手段と、前記変換信号の送受信動作に先立って、前記通信手段を介して、自機の固有の識別情報を前記他の電子機器に送信し、前記他の電子機器の固有の識別情報を受信する制御手段と、を備えることを特徴とする。

【0025】このように、ユーザは、任意の場所から他の電子機器に対して、内部に記憶するデータを変換して送信する。これにより、このデータの送信時にデータが盗まれた場合にも、データを解読することは困難となるので、より安全性の高い信号として送信することができる。

【0026】請求項8の発明は、請求項7において、前記変換信号は、暗号化信号であることを特徴とする。

【0027】データは、前記KPSによって、前記他の電子機器の固有の識別情報及び自機の固有の秘密アルゴリズムを用いて暗号化されており、この暗号化されたデータは、前記携帯型通信装置の固有の識別情報及び前記他の電子機器の固有の秘密アルゴリズムを用いなければ、復号化することは困難であるので、送信時のデータの安全性を高めることができる。

【0028】請求項9の発明は、請求項8において、前記変換手段は、前記他の電子機器の固有の識別情報及び自機の固有の秘密アルゴリズムを用いて暗号鍵を生成し、この暗号鍵を用いた暗号鍵プログラムにより前記データを暗号化する暗号化手段であることを特徴とする。

【0029】これにより、データを送信するときに、前記固有の識別情報及び前記固有の秘密アルゴリズムを用いて、前記KPSによるデータの暗号化を行うことができる。

【0030】このKPSにより暗号化されたデータは、その送信時に盗まれた場合にも、前記暗号鍵を使用しなければ、復号化することは困難であるので、送信時のデータの安全性を高めることができる。

【0031】請求項10の発明は、請求項8、9のいずれかにおいて、前記変換手段は、前記他の電子機器から送信された暗号化信号を、前記他の電子機器の固有の識別情報及び自機の固有の秘密アルゴリズムを用いて復号化する復号化手段を含むことを特徴とする。

【0032】これにより、前記KPSを用いて暗号化されたデータの暗号化信号を、復号化して、元のデータを復元することができる。

【0033】請求項11の発明は、請求項10において、前記復号化手段は、前記他の電子機器の固有の識別情報及び自機の固有の秘密アルゴリズムを用いて暗号鍵を生成し、この暗号鍵を用いた暗号鍵プログラムにより信号を復号化することを特徴とする。

【0034】前記KPSに用いた復号化を行う際に用いる暗号鍵を、前記送信された他の電子機器の固有の識別

情報及び自機の固有の秘密アルゴリズムを用いて生成するので、前記暗号鍵を簡易に生成することができる。

【0035】請求項12の発明は、請求項10、11のいずれかにおいて、前記制御手段は、前記暗号化手段で前記記憶手段に記憶するデータを暗号化して暗号化信号を生成し、この暗号化信号を前記通信手段を介して前記他の電子機器に送信した後、前記他の電子機器で処理されたデータを暗号化した暗号化信号を前記通信手段で受信して、前記復号化手段で復号化することを特徴とする。

【0036】これにより、記憶するデータを処理速度の速い他の電子機器で迅速に処理することができる。このとき、前記データを暗号化信号に変換して送信するので、前記データの送信時に、前記データを盗まれた場合にも、前記データを解読することが困難となり、データの安全性を高めることができる。

【0037】請求項13の発明は、請求項10～12のいずれかに記載する携帯型記憶装置を備えて成る携帯型電話装置であることを特徴とする。

【0038】このように、1つの電子機器が、携帯型記憶装置の機能及び携帯型電話装置の機能を備えるので、ユーザは、2つの電子機器をそれぞれ携帯する必要がなくなり、多機能の電子機器を簡易に携帯することができる。

【0039】

【発明の実施の形態】次に、本発明の好適な実施の形態を説明する。

【0040】図1は、本発明に係る携帯型通信装置を含む携帯型記憶装置の概略的な構成を示す。

【0041】まず、携帯型記憶装置1の第1の実施の形態について、以下に説明する。

【0042】この図1の携帯型記憶装置1は、人が携帯して利用可能な大きさであり、他の電子機器と情報を送受信する通信手段である通信制御部22と、前記他の電子機器の固有の識別情報及び自機の固有の秘密アルゴリズムを用いてデータを変換し、前記通信手段を介して前記変換したデータによる変換信号を前記他の電子機器に送信する変換手段である暗号化／復号化部20と、前記変換信号の送受信動作に先立って、前記通信手段を介して、自機の固有の識別情報を前記他の電子機器に送信し、前記他の電子機器の固有の識別情報を受信する制御手段である制御部10とを備える。

【0043】また、この携帯型記憶装置1は、ユーザの操作により、命令や情報を入力する入力部14と、制御部10で制御されるデータ等を表示する表示部16とを備える。前記入力部14は、キーボードやペン等の入力操作を行うことができるものである。前記表示部16は、液晶パネル等を用いたディスプレイ装置である。また、タッチパネルを用いることにより、前記入力部14を前記表示部16上に設けることも可能である。

【0044】さらに、この携帯型記憶装置1は、データを記憶する、大容量の記憶手段である記憶部12を備える。これにより、携帯型記憶装置1の内部の記憶部12に記憶されるデータを他の電子機器に送信することができる。

【0045】この記憶部12のデータを他の電子機器に送信するときには、制御部10の制御により、記憶部12のデータが読み出されて、暗号化／復号化部20に送られる。このデータは、暗号化／復号化部20で暗号化される。この暗号化されたデータは、通信制御部22の制御により、暗号化信号として、他の電子機器に送信される。また、他の電子機器から送信される暗号化信号は、通信制御部22で受信されて、暗号化／復号化部20に送られる。この暗号化／復号化部20では、暗号化信号を復号化する。これにより、復号化されたデータは、制御部10の制御により、記憶部12に記憶される。

【0046】次に、携帯型記憶装置1と他の複数の電子機器とがワイヤレスで信号を送受信する通信システムの概略的な構成を、図2に示す。

【0047】この携帯型記憶装置1は、例えば、ファクシミリ装置301や、いわゆるタワー型のコンピュータ装置302や、高性能な大型コンピュータ装置303や、いわゆるハンドヘルド・コンピュータ装置304や、プロジェクタ装置305や、ノートブック型のパーソナルコンピュータ装置（以下、PCという）306等の様々な電子機器と、ワイヤレスに暗号化信号の送受信を行う。

【0048】携帯型記憶装置1から送信される暗号化信号を受信した電子機器は、前記暗号化信号を復号化して元のデータを復元し、このデータを印刷したり、処理したりする。

【0049】このデータの暗号化／復号化方法としては、電子情報通信学会論文誌 A Vol. J71-A No. 11 p. 2046-2053 1988年11月に掲載される、暗号鍵を通信なしで共有する方法：KEY PREDISTRIBUTION SYSTEM（以下、KPSという）を用いる。このKPSを用いたデータの暗号化／復号化方法では、データを暗号化及び復号化するときに用いる暗号鍵を、データを送受信する電子機器間で予め共有しておき、データを送信する電子機器では、前記暗号鍵を用いてデータを暗号化し、データを受信する電子機器では、受信した暗号化信号を前記暗号鍵を用いて復号化する。

【0050】このKPSで用いる暗号鍵を生成するために、携帯型記憶装置1、ファクシミリ装置301、タワー型のコンピュータ装置302、高性能な大型コンピュータ装置303、ハンドヘルド・コンピュータ装置304、プロジェクタ装置305、及びPC306は、固有の識別情報（以下、固有のIDという）及び固有の秘密アルゴリズムをそれぞれ備える。具体的には、携帯型記

憶装置 1 は、暗号化／復号化部 20 内に備えるメモリ等に、固有の ID 及び固有の秘密アルゴリズムを記憶する。

【0051】前記通信システム内の 2 つの電子機器で、信号を送受信するときには、まず、固有の ID を相互に送受信して、信号を送信すべき電子機器の固有の ID を記憶する。次に、信号を送信する一方の電子機器は、前記受信した他方の電子機器の固有の ID 及び自機の固有の秘密アルゴリズムを用いて暗号鍵を生成し、この暗号鍵を用いた暗号鍵プログラムによりデータを暗号化する。そして、この暗号化したデータによる暗号化信号を、他方の電子機器に送信する。また、他方の電子機器も、前記受信した一方の電子機器の固有の ID 及び固有の秘密プログラムを用いて暗号鍵を生成し、この暗号鍵を用いた暗号鍵プログラムにより、受信した暗号化信号を復号化して元のデータを復元する。

【0052】次に、前記通信システムのうちの、携帯型記憶装置 1 とプリンタ装置 301 との通信について説明する。

【0053】プリンタ装置 301 は、データを印刷する出力部 604 と、他の電子機器との間で信号を送受信する通信部 700 と、ID 記憶部 710 と、前記各部の動作を制御する制御部 602 とを備える。

【0054】通信部 700 は、暗号化／復号化部 702 及び通信制御部 704 を備える。この前記暗号化／復号化部 702 は、携帯型記憶装置 1 の暗号化／復号化部 20 と同様の機能を備え、通信制御部 704 は携帯型記憶装置 1 の通信制御部 22 と同様の機能を備える。ID 記憶部 710 は、このプリンタ装置 301 の固有の ID 及び固有の秘密アルゴリズムが記憶された IC である。

【0055】まず、携帯型記憶装置 1 の固有の ID 及びプリンタ装置 301 の固有の ID の送受信について説明する。

【0056】携帯型記憶装置 1 は、制御部 10 の制御により、プリンタ装置 301 に対して、プリンタ装置 301 の固有の ID の送信要求命令を送信する。

【0057】プリンタ装置 301 は、前記固有の ID の送信要求命令を通信制御部 704 で受信する。この受信した固有の ID の送信要求命令は、制御部 602 に送られる。制御部 602 は、前記受信した固有の ID の送信要求命令に応じて、通信部 700 を制御する。通信部 700 は、ID 記憶部 710 から固有の ID を読み出す。このプリンタ装置 301 の固有の ID は、通信制御部 704 の制御により、携帯型記憶装置 1 に送信される。

【0058】携帯型記憶装置 1 は、前記送信されたプリンタ装置 301 の固有の ID を、通信制御部 22 で受信し、暗号化／復号化部 20 に記憶する。また、暗号化／復号化部 20 は、この携帯型記憶装置 1 の固有の ID を読み出す。この固有の ID は、通信制御部 504 の制御により、プリンタ装置 301 に送信される。

【0059】プリンタ装置 301 は、前記送信された携帯型記憶装置 1 の固有の ID を、通信制御部 704 で受信して、記憶する。

【0060】次に、データの暗号化及び復号化について説明する。

【0061】固有の ID の送受信後、携帯型記憶装置 1 の暗号化／復号化部 20 では、プリンタ装置 301 の固有の ID 及び自機の固有の秘密プログラムを用いて暗号鍵を生成する。

10 【0062】例えば、携帯型記憶装置 1 の記憶部 12 に記憶されているデータを送信するときには、制御部 10 からの制御により、前記記憶部 12 に記憶されるデータが、暗号化／復号化部 20 に送られる。暗号化／復号化部 20 では、前記生成した暗号鍵を用いた暗号鍵プログラムにより、前記送られたデータを暗号化する。この暗号化された暗号化信号は、通信制御部 22 の制御により、プリンタ装置 301 に送信される。

20 【0063】携帯型記憶装置 1 から送信された暗号化信号は、プリンタ装置 301 の通信制御部 704 で受信されて、暗号化／復号化部 702 に送られる。この暗号化／復号化部 702 では、前記受信した携帯型記憶装置 1 の固有の ID 及び自機の固有の秘密プログラムを用いて暗号鍵を生成する。そして、この暗号鍵を用いた暗号鍵プログラムにより、前記受信した暗号化信号を復号化する。これにより、暗号化される前のデータが復元される。この復元された元のデータは、制御部 602 の制御により、出力部 604 に送られる。そして、出力部 604 により、データが印刷されて出力される。

30 【0064】このように、携帯型記憶装置 1 とプリンタ装置 301 との間では、記憶部 12 に記憶されるデータを暗号化して送信し、受信した暗号化信号を復号化する。

【0065】ここで、従来のデータの暗号化方式では、データを暗号化するとき用いる暗号鍵及び暗号化データを復号化するとき用いる復号鍵は、例えば、暗号鍵及び復号鍵を管理する管理システム等から通信によって配送されることにより得ている。これに対して、KPS を用いたデータの暗号化／復号化を行うことにより、携帯型記憶装置 1 及びプリンタ装置 301 は、暗号鍵及び復号鍵を内部で生成するので、前記暗号鍵及び復号鍵を簡易に得ることができる。また、前記管理システムを設置する必要がなく、前記管理システムの設備にかかる費用等を削減することができる。さらに、暗号化したデータが、その送信中に第三者に傍受されて盗まれた場合にも、その暗号化したデータを解読することは困難であるので、データの安全性を保つことができる。

50 【0066】尚、固有の ID として、携帯型記憶装置 1 のユーザの名前、電話番号、電子メールのアドレス等の、データを送受信する電子機器間で予め知っている情報を用いることにより、固有の ID を予め用意する必要

がなくなるので、データの暗号化／復号化をさらに簡易に行うことができる。

【0067】次に、携帯型記憶装置1のデータをプリンタ装置301で印刷するときの、携帯型記憶装置1とプリンタ装置301との信号の送受信の手順について、図3のフローチャートを用いて説明する。

【0068】まず、ステップS2で、携帯型記憶装置1では、記憶部12に記憶するデータのファイル名を、入力部14を操作して指定する。

【0069】次に、ステップS4で、ユーザは、入力部14を操作して、表示部16に表示される印刷コマンド等を選択する。この入力命令は、制御部10に送られる。

【0070】このとき、ステップS22で、プリンタ装置301は、電源がONであってプリント可能な状態、いわゆるスタンバイ状態となっているものとする。

【0071】次に、ステップS6で、携帯型記憶装置1の制御部10は、プリンタ装置301に対して、IDの送信要求命令を送信する。

【0072】ステップS24で、プリンタ装置301は、前記IDの送信要求命令を受信し、このIDの送信要求命令に応じて、固有のIDを携帯型記憶装置1に送信する。

【0073】携帯型記憶装置1は、プリンタ装置301から送信されるプリンタ装置301の固有のIDを受信して記憶する。また、携帯型記憶装置1は、自機の固有のIDをプリンタ装置301に送信する。

【0074】プリンタ装置301は、携帯型記憶装置1の固有のIDを受信して記憶する。

【0075】この後、ステップS12で、携帯型記憶装置1は、プリンタ装置301の固有のID及び自機の固有の秘密プログラムを用いて暗号鍵を生成する。また、ステップS26で、プリンタ装置301は、携帯型記憶装置1の固有のID及び自機の固有の秘密アルゴリズムを用いて暗号鍵を生成する。

【0076】次に、ステップS14で、携帯型記憶装置1は、生成した暗号鍵を用いた暗号鍵プログラムにより、印刷用のデータを暗号化する。そして、この暗号化した印刷用データ及びこの印刷用データを印刷するときの制御用データである印刷制御用コードをプリンタ装置301に送信する。

【0077】一方、ステップS28で、プリンタ装置301は、暗号化された印刷用データ及び印刷制御用コードを受信する。

【0078】そして、ステップS30で、暗号化された印刷用データを復号化して、元の印刷用データを復元する。この後、受信した印刷制御用コードに基づいて、印刷用データを印刷する。また、印刷が正常に行われたか否か等を示す印刷制御用コードを、携帯型記憶装置1に対して送信する。携帯型記憶装置1は、プリンタ装置3

01からの印刷制御用コードを受信し、この印刷制御用コードに基づいて、プリンタ装置301で印刷が正常に行われたか否かを判別する。

【0079】次に、携帯型記憶装置1の第2の実施の形態について説明する。

【0080】この携帯型記憶装置1は、着脱自在に装着され、固有の識別情報、固有の秘密アルゴリズム、及びデータを記憶する携帯型記憶媒体と、前記携帯型記憶媒体から前記固有の識別情報、前記固有の秘密アルゴリズム、及び前記データを読み出す情報入力手段である情報入力部18とを含む。この携帯型記憶媒体としては、例えばICカードを用いることができる。

【0081】この携帯型記憶装置1が他の電子機器と信号を送受信するときにも、まず、固有のIDを他の電子機器と送受信した後に、信号を送信する側である携帯型記憶装置1ではデータを暗号化して送信し、信号を受信する側である他の電子機器では、送信された暗号化信号を復号化してデータを復元する。

【0082】まず、制御部10の制御により、情報入力部18に装着される前記携帯型記憶媒体から、自機の電子機器の固有のID、自機の固有の秘密プログラム、及びデータが読み出される。前記自機の電子機器の固有のIDは、制御部10の制御により、通信制御部22を介して他の電子機器に送信される。また、他の電子機器の固有のIDを、通信制御部22で受信して、記憶する。

【0083】この後、携帯型記憶装置1は、前記自機の固有の秘密プログラム及びデータを、暗号化／符号化部20に送る。この暗号化／符号化部20は、前記他の電子機器の固有のID及び自機の固有の秘密プログラムを用いて暗号鍵を生成し、この暗号鍵を用いた暗号鍵プログラムにより前記データを暗号化する。この暗号化信号は、通信制御部22を介して他の電子機器に送信される。

【0084】また、暗号化信号を受信したときには、暗号化信号は、通信制御部22を介して暗号化／復号化部20に送られる。暗号化／復号化部20は、前記暗号化信号を、前記暗号鍵を用いた暗号鍵プログラムにより復号化して、データを復元する。この復元されたデータは、制御部10の制御により、前記携帯型記憶媒体に書き込まれる。

【0085】例えば、図4に示すように、携帯型記憶装置1には、情報入力部18であるICカード挿入部が設けられ、このICカード挿入部に携帯型記憶媒体であるICカード101を挿入するものである。この携帯型記憶装置1は、コンピュータ装置100と、前記ICカード101に記憶されるデータを送受信する。

【0086】具体的には、例えば、ICカード101は、ネットワークを通じた電子商取引（エレクトロニクス・コマース：electronic commerce）において、電子的な決済に用いるプリペイドカードや、キャッシュカー

ドや、クレジットカード等とすることが考えられる。このとき、前記コンピュータ装置100は、例えば、複数のコンピュータ装置等が相互に接続されたネットワークであって、商業的な取引が行われる、いわゆるサイバーモールに接続される端末となる。

【0087】携帯型記憶装置1のICカード101には、IC102が組み込まれている。

【0088】このIC102に、自機の固有のID、自機の固有の秘密アルゴリズム及びデータが記憶される。携帯型記憶装置1の制御部10は、前記自機の固有のIDを読み出して、通信制御部22を介してコンピュータ装置100に送信し、また、コンピュータ装置100の固有のIDを受信する。

【0089】携帯型記憶装置1の制御部10は、前記自機の固有の秘密アルゴリズムをICカード101のIC102から読み出し、この自機の固有の秘密アルゴリズムを暗号化／復号化部20に送る。暗号化／復号化部20は、この自機の固有の秘密アルゴリズムと前記コンピュータ装置100の固有のIDとを用いて暗号鍵を生成する。さらに、携帯型記憶装置1の制御部10は、IC102からデータを読み出し、このデータを暗号化／復号化部20に送る。暗号化／復号化部20は、前記データを前記暗号鍵を用いた暗号鍵プログラムで暗号化する。この暗号化されたデータは、暗号化信号として通信制御部22を介してコンピュータ装置100に送信される。

【0090】このコンピュータ装置100は、暗号化信号を受信したときには、携帯型記憶装置1の固有のID及び自機の固有の秘密アルゴリズムを用いて暗号鍵を生成し、この暗号鍵を用いた暗号鍵プログラムで前記暗号化信号を復号化する。そして、コンピュータ装置100は、復号化された元のデータを処理する。このとき、必要に応じて、前記データをサイバーモール内の他のコンピュータ装置に送信して処理する場合もある。この後、コンピュータ装置100は、前記処理されたデータを暗号化し、この暗号化信号を携帯型記憶装置1に送信する。

【0091】携帯型記憶装置1は、前記暗号化信号を通信制御部22で受信し、暗号化／復号化部20に送る。前記暗号化信号は、この暗号化／復号化部20で前記暗号鍵を用いた暗号鍵プログラムにより復号化されて、データが復元される。この復元されたデータは、制御部10の制御により、ICカード101のIC102に書き込まれる。

【0092】例えば、ICカード101をプリペイドカードとして用いるときには、ICカード101のIC102に記憶されるデータは現金の残高である。よって、ユーザが購入した物の代金を前記ICカード101を用いて支払うときには、携帯型記憶装置1でICカード101に記憶される金額を読み出して、コンピュータ

装置100に送信する。コンピュータ装置100は、送信された残高から前記購入物の代金分を減算し、この減算した金額のデータを携帯型記憶装置1に送信する。携帯型記憶装置1は、前記送信された金額をICカード101のIC102に書き込む。

【0093】このように、ユーザは、所有するICカード101を、不特定多数のユーザが使用するコンピュータ装置100に直接に装着せずに、自分が所有する携帯型記憶装置1にICカード101を装着して、このICカード101を利用することができる。また、ICカード101のデータをコンピュータ装置100に送信するときに、ICカード101のデータをKPSを用いた暗号化方法で暗号化するので、この暗号化されたデータが盗まれた場合にも、このデータを他人に盗用されることを防止できる。

【0094】次に、携帯型記憶装置1に記憶するデータ等を他の電子機器に送信し、そのデータを前記他の電子機器内で処理し、その処理されたデータ等を受信して記憶するデータ処理、いわゆる依頼計算処理について説明する。

【0095】例えば、図5に示すように、携帯型記憶装置1では、計算処理用のデータ及び計算処理プログラムを暗号化し、この暗号化されたデータ及び計算処理プログラムを計算情報としてPC306に送信する。PC306では、暗号化されたデータ及び計算処理プログラムを受信して復号化する。そして、復号化された元の計算処理プログラムを用いて、復号化した元のデータを計算処理する。この後、計算処理されたデータ及び計算処理プログラムを暗号化して、計算実行結果として携帯型記憶装置1に送信する。携帯型記憶装置1では、この計算実行結果を受信して、復号化する。これにより、計算処理されたデータ及び計算処理プログラムを復元し、このデータ及び計算処理プログラムを記憶する。

【0096】このように、携帯型記憶装置1は、データ等を他の電子機器に送信して、その他の電子機器の処理能力を借りてデータ処理を行う。このとき、前記他の電子機器が高速な処理能力を備えたコンピュータ装置であるならば、携帯型記憶装置1を所有するだけで、より迅速なデータ処理を行うことができる。

【0097】また、携帯型記憶装置1と他の電子機器の間のデータの送受信時には、KPSを用いた暗号化方法によりデータを暗号化して送受信する。このKPSによる暗号化データを盗んでも、復号鍵を持たなければ、暗号化データを復号化することは困難であるので、送受信時のデータの安全性を高めることができる。

【0098】尚、計算処理プログラム以外のアプリケーションプログラムを用いて、計算処理以外のデータ処理を行うことも可能である。

【0099】また、PC306内に所望の計算処理プログラム等のアプリケーションプログラムが記憶されてい

ることが、予め判明しているならば、このアプリケーションプログラムを送信する必要はない。

【0100】上述したデータ処理を行うには、例えば、携帯型記憶装置1の記憶部12を、PC306に接続されたハードディスクドライブ装置とみなし、この記憶部12に記憶されるデータを処理する。

【0101】このときの信号の送受信の手順を、図6のフローチャートを用いて説明する。

【0102】まず、ステップS42で、携帯型記憶装置1は、PC306から送信されるデータの受信可能な状態である、いわゆるスタンバイ状態となっているものと  
10

【0103】一方、ステップS62で、PC306は、任意の携帯型記憶装置をPC306に接続される記憶装置、即ちハードディスクドライブ装置のうちの1つとみなすことができる状態となっている。

【0104】これにより、ステップS64で、PC306のディスプレイ部には、接続可能な携帯型記憶装置の一覧表、いわゆるリストが表示される。尚、この場合には、携帯型記憶装置は1つであるので、前記リストには  
20 前記携帯型記憶装置1しか表示されない。よって、ユーザは前記携帯型記憶装置1を選択する。この選択により、PC306から携帯型記憶装置1に対して、PC306のハードディスクドライブ装置として選択したことを示す命令が送信される。

【0105】携帯型記憶装置1は、ステップS44で、PC306から送信された選択命令を受信する。そして、携帯型記憶装置1は、PC306からドライブ装置として選択されたことを、表示部16に表示する。

【0106】ユーザは、携帯型記憶装置1をPC306のハードディスクドライブ装置のうちの1つに設定する  
30 可否かを決定する。この決定情報は、PC306に送信される。

【0107】このように、携帯型記憶装置1側で、PC306のハードディスクドライブ装置のうちの1つとなることを設定する可否かを決定する。従って、PC306の選択のみによって携帯型記憶装置1をハードディスクドライブ装置と設定し、携帯型記憶装置1に記憶されるデータを強制的に受信すること、即ち携帯型記憶装置1のデータを盗むことを防止できる。

【0108】この後、ステップS46で、携帯型記憶装置1は、PC306に対して、IDの送信要求命令を送信する。

【0109】PC306は、ステップS66で、前記IDの送信要求命令を受信し、このIDの送信要求命令に応じて、固有のIDを携帯型記憶装置1に送信する。

【0110】携帯型記憶装置1は、PC306から送信されるPC306の固有のIDを受信して記憶する。また、携帯型記憶装置1は、自機の固有のIDをPC306に送信する。よって、PC306は、携帯型記憶装置  
50

1の固有のIDを受信して記憶する。

【0111】この後、ステップS48で、携帯型記憶装置1は、PC306の固有のID及び自機の固有の秘密プログラムを用いて暗号鍵を生成する。

【0112】また、ステップS68で、PC306は、携帯型記憶装置1の固有のID及び自機の固有の秘密アルゴリズムを用いて暗号鍵を生成する。

【0113】次に、ステップS50で、携帯型記憶装置1は、生成した暗号鍵を用いた暗号鍵プログラムにより、任意のファイルのデータを暗号化する。そして、この暗号化したデータを、暗号化信号としてPC306に送信する。

【0114】PC306では、ステップS70で、送信された暗号化信号を受信して、復号化する。この復号化により復元されたデータは、ユーザによるアプリケーションソフトウェア上の作業により、処理される。

【0115】そして、PC306は、ステップS72で、前記生成した暗号鍵を用いた暗号鍵プログラムにより、前記処理データを暗号化する。PC306は、この暗号化されたデータを携帯型記憶装置1に送信する。

【0116】携帯型記憶装置1は、ステップS52で、送信された暗号化信号データを受信して、復号化する。これにより、復元された処理データは、記憶部12に記憶される。

【0117】この後、ステップS54で、携帯型記憶装置1では、PC306のハードディスクドライブ装置となることが解除されて、PC306との接続が切断される。

【0118】一方、PC306でも、ステップS74で、携帯型記憶装置1をハードディスクドライブ装置のうちの1つとして設定することが解除されて、携帯型記憶装置1との接続が切断される。

【0119】さらに、上述した携帯型記憶装置の構成を、携帯型電話装置に備えることもできる。これにより、ユーザは、携帯型電話装置のみを携帯することで、電話通信の他に、データの送受信や処理等を行うことができる。

【0120】

【図面の簡単な説明】

【図1】本発明に係る携帯型通信装置を含む携帯型記憶装置の第1の実施の形態及びプリンタ装置の概略的な構成図である。

【図2】携帯型記憶装置と他の電子機器との信号の送受信を説明するための図である。

【図3】携帯型記憶装置とプリンタ装置との信号の送受信の手順を示すフローチャートである。

【図4】携帯型記憶装置の第2の実施の形態及びその具体的な実施例について説明するための図である。

【図5】携帯型記憶装置の他の実施例について説明するための図である。

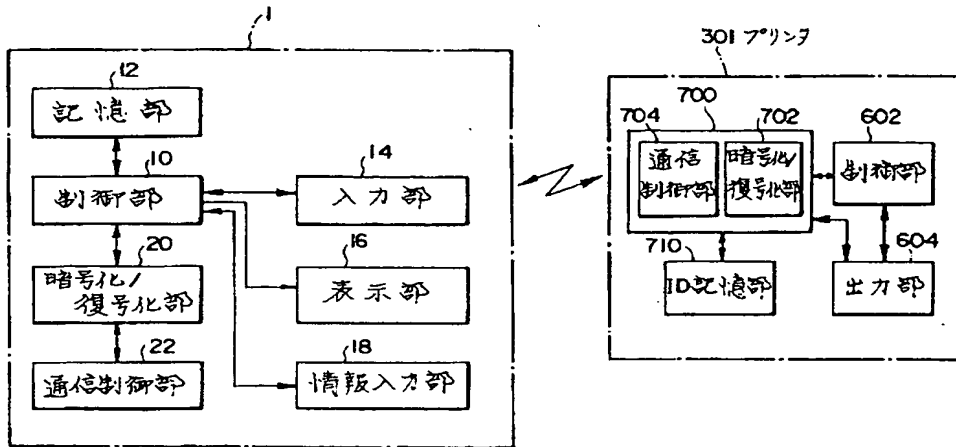
【図6】携帯型記憶装置とPCとの信号の送受信の手順を示すフローチャートである。

【符号の説明】

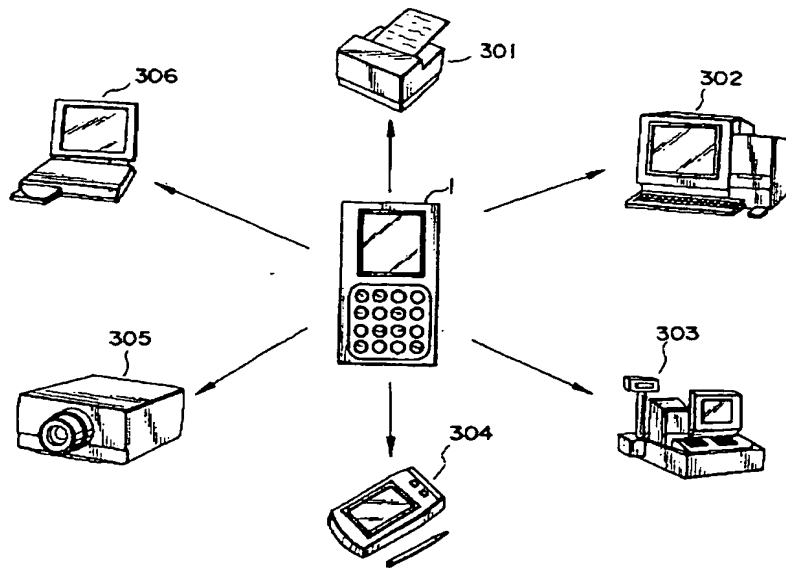
- 1 携帯型記憶装置
- 10 制御部
- 12 記憶部

- 14 入力部
- 16 表示部
- 18 情報入力部
- 20 暗号化／復号化部
- 22 通信制御部

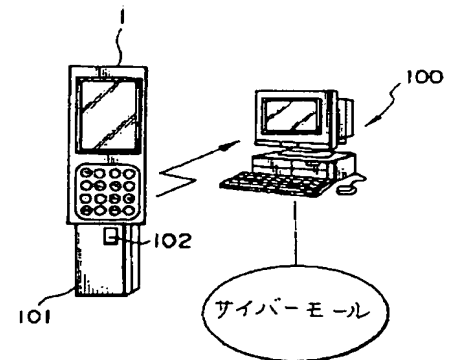
【図1】



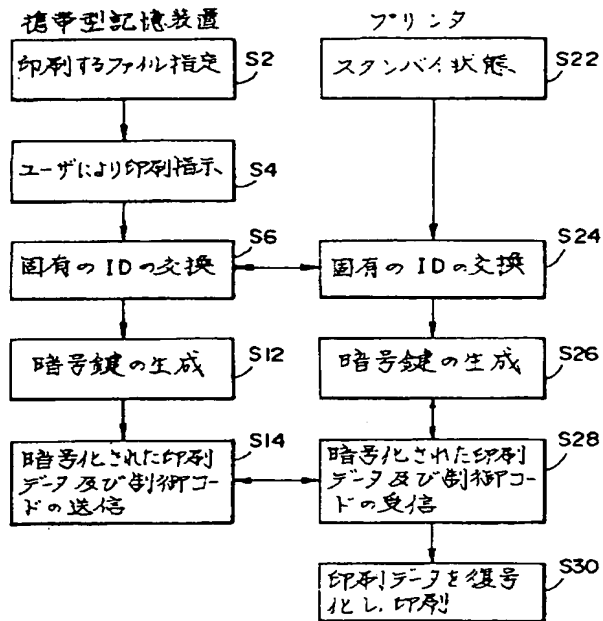
【図2】



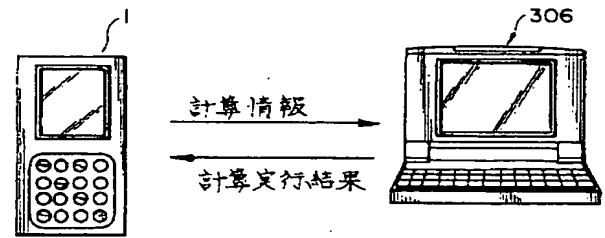
【図4】



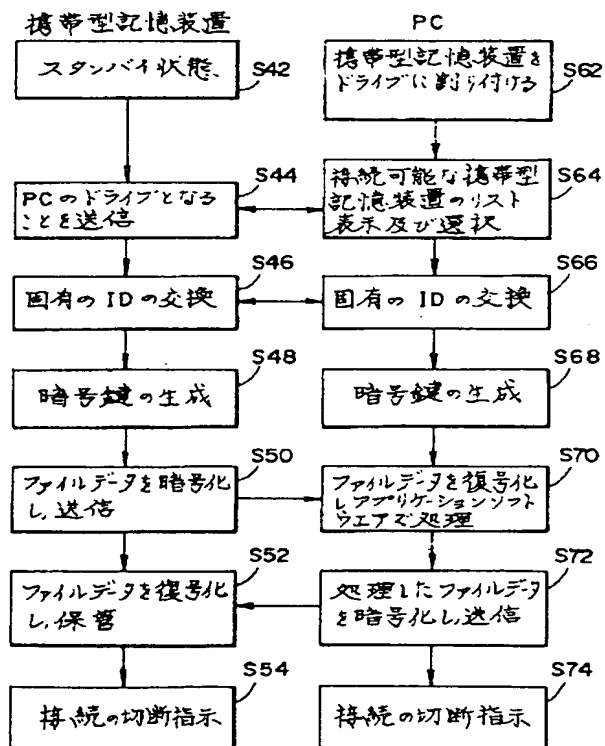
【図3】



【図5】



【図6】





フロントページの続き

(51) Int. Cl. <sup>6</sup>	識別記号	庁内整理番号	F I	技術表示箇所
// G 0 6 F 12/14	3 2 0		H 0 4 L 9/00	6 0 1 D